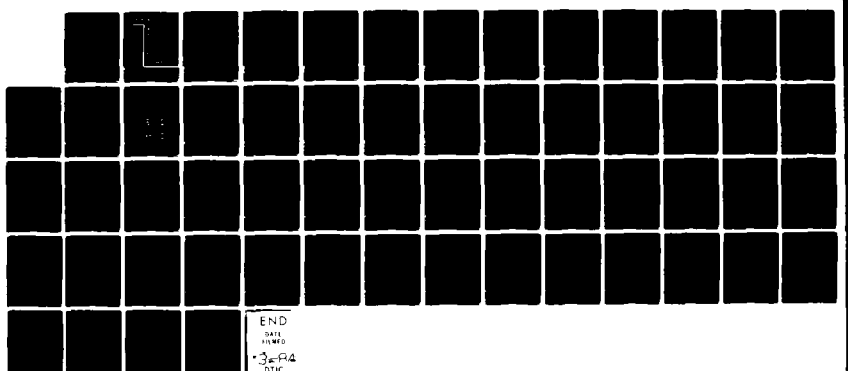
AD A137 456 LOGISTICS ENGINEERING DESIGN TECHNIQUES FOR FAULT-TOLERANT AVIONICS SYSTEMS(U) ANALYTIC SCIENCES CORP READING MA M H VEATCH ET AL. JAN 84 1/1

UNCLASSIFIED AFHRL-TP-83-41 F33615-82-C-0002 F/G 15/5 NL

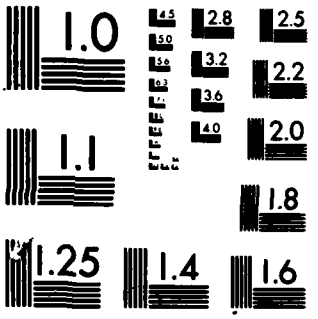


END

DATE FILMED

3-84

DTIC



AFHRL-TP-83-41

(12)

AIR FORCE HUMAN RESOURCES LABORATORY

LOGISTICS ENGINEERING DESIGN TECHNIQUES FOR FAULT-TOLERANT AVIONICS SYSTEMS

By

Michael H. Veatch
Alberto B. Calvo

The Analytic Sciences Corporation
One Jacob Way
Reading, Massachusetts 01867

James C. McManus

LOGISTICS AND HUMAN FACTORS DIVISION
Wright-Patterson Air Force Base, Ohio 45433

January 1984

Interim Paper for Period April 1982–July 1983

AIR FORCE SYSTEMS COMMAND
BROOKS AIR FORCE BASE, TEXAS 78235

NOTICE

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely Government-related procurement, the United States Government incurs no responsibility or any obligation whatsoever. The fact that the Government may have formulated or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication, or otherwise in any manner construed, as licensing the holder, or any other person or corporation; or as conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

The Public Affairs Office has reviewed this paper, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This paper has been reviewed and is approved for publication.

JOSEPH A. BIRT, Lt Col, USAF
Technical Director
Logistics and Human Factors Division

DONALD C. TETMEYER, Colonel, USAF
Chief, Logistics and Human Factors Division

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: AFHRL-TP-83-41

2. GOVT ACCESSION NO: A137456

3. RECIPIENT'S CATALOG NUMBER

4. TITLE *(and Subtitle)*

LOGISTICS ENGINEERING DESIGN TECHNIQUES FOR FAULT-TOLERANT AVIONICS SYSTEMS

5. TYPE OF REPORT & PERIOD COVERED
Interim
April 1982 to July 1983

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Michael H. Veatch
Alberto B. Calvo
James C. McManus

8. CONTRACT OR GRANT NUMBER(s)
F33615-82-C-0002

9. PERFORMING ORGANIZATION NAME AND ADDRESS
The Analytic Sciences Corporation
One Jacob Way
Reading, Massachusetts 01867

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
62205F
17100026

11. CONTROLLING OFFICE NAME AND ADDRESS
HQ Air Force Human Resources Laboratory (AFSC)
Brooks Air Force Base, Texas 78235

12. REPORT DATE
January 1984

13. NUMBER OF PAGES
60

14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)*
Logistics and Human Factors Division
Air Force Human Resources Laboratory
Wright-Patterson Air Force Base, Ohio 45433

15. SECURITY CLASS *(of this report)*
Unclassified

15.a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of this abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

communication
fault-tolerant avionics
identification
logistics analysis
mean time between critical failures
mean time between failures
mean time to repair
mission completion success probability

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

The logistics analysis methods in this paper are appropriate for integrated, fault-tolerant systems, such as the Integrated Communication, Navigation, Identifications Avionics (ICNIA) program, early in the development cycle. In particular, fault tolerance is one feature that an ICNIA system must have if reliability and supportability cost benefits are to be realized.

DD Form 1473 EDITION OF 1 NOV 65 IS OBSOLETE
1 Jan 73

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

Item 19 (*Continued*)

Mission Reliability Model (MIREM)
navigation
reliability and maintainability
Simulation of Operational Availability/Readiness (SOAR) model
supportability

Item 20 (*Continued*)

Historically, logistics engineering disciplines have been applied to new avionics designs in the later stages of development. However, the logistics engineering techniques in the early stages of design should not impose unrealistically detailed data requirements for analysis. This research in the areas of reliability, supportability, and survivability proceeded by front-end analysis to determine the applicability of existing techniques. Both traditional and innovative maintenance concepts were investigated. In particular, the increased ability to sustain sorties with limited repair capability was evaluated for deferred repair policies. A detailed example is presented to demonstrate the reliability and supportability methodologies.

The outputs of this research in each area consists of documented methods for evaluation of integrated, fault-tolerant designs and the associated logistics options, as well as specific evaluations and design feedback for the ICNIA designs. The Mission Reliability Model (MIREM) was developed to determine the reliability of avionics designs in the early stages of development while the Simulation of Operational Availability/Readiness (SOAR) model was extended to describe the supportability parameters of the designs.

AFHRL Technical Paper 83-41 January 1984

LOGISTICS ENGINEERING DESIGN TECHNIQUES FOR FAULT-TOLERANT AVIONICS SYSTEMS

By

Michael H. Veatch
Alberto B. Calvo

The Analytic Sciences Corporation
One Jacob Way
Reading, Massachusetts 01867

James C. McManus

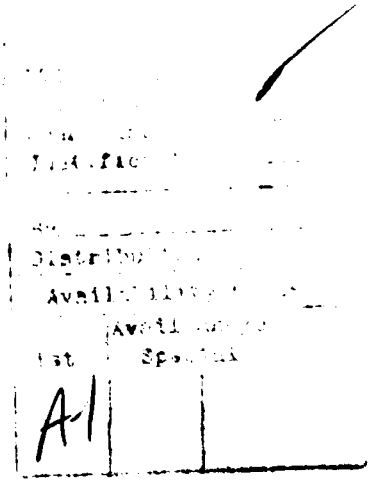
LOGISTICS AND HUMAN FACTORS DIVISION
Wright-Patterson Air Force Base, Ohio 45433

Reviewed by

Michel A. King, Captain, USAF
Chief, Logistics Systems Branch

Submitted for publication by

Donald C. Tetmeyer, Colonel, USAF
Chief, Logistics and Human Factors Division



PREFACE

This work is currently supported by the Air Force Human Resources Laboratory and Air Force Wright Aeronautical Laboratories at Wright-Patterson Air Force Base under Contract Number F33615-82-C-0002, Impact Analysis of ICNIA. The guidance and support of Mr. James C. McManus and Mr. Robert L. Harris of these organizations are greatly appreciated. The methodologies developed in this report to analyze reliability and supportability of integrated, fault-tolerant avionics will be applied to specific ICNIA architectures in additional reports prepared under this contract.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

The growing requirement for tactical aircraft Communication, Navigation and Identification (CNI) avionics in the presence of volume, weight, power and cost constraints is currently forcing avionics designers to consider system integration (Reference 1). Fault tolerance is one feature that an Integrated CNI Avionics (ICNIA) system must have if reliability and support cost benefits are to be realized. Exploring the reliability, supportability and survivability implications of an integrated, fault-tolerant architecture requires new techniques (Reference 2).

Historically, logistics engineering disciplines have been applied to new avionics designs in the later stages of development. To ensure that avionics designs are reliable, supportable and survivable in the operating environment, logistics engineering techniques are needed that can be effectively implemented during the advanced design phase of the system development cycle. Techniques employed in this phase will challenge design engineers to provide logistics support, reliability and survivability capabilities before the design is fixed. In particular, logistics engineering techniques are needed that do not impose unrealistic detailed data requirements during the earlier stages of design.

The combination of these two factors creates a need for new and innovative logistics engineering techniques. The need currently exists in the two ICNIA system development programs that are being pursued at the Air Force Wright Aeronautical Laboratories (AFWAL). One program (System A) uses agile bandpass filter technology, and the other (System B) employs analog large scale integration technology.

1.2 OVERVIEW

The logistics analysis methods presented in this paper are appropriate for integrated, fault-tolerant systems, such as ICNIA, early in the development cycle. Traditional and innovative maintenance concepts are investigated. In particular, the increased ability to sustain sorties with limited repair capability is evaluated for deferred repair policies. A detailed example is presented to demonstrate the reliability and supportability methodology.

These techniques were developed under the Impact Analysis of ICNIA Program. The program has the following additional goals:

1. Apply these techniques to the two ICNIA architectures under development.

2. Influence the ICNIA designs to improve reliability, supportability and survivability.

3. Document the research and development results in a form amenable for use by design engineers.

An overview of the Impact Analysis of ICNIA Program is shown in Figure 1. Research in the reliability, supportability and survivability areas was preceded by front-end analyses to determine the applicability of existing techniques. The output of the research in each area consists of documented methods for evaluation of integrated, fault-tolerant designs and the associated logistics options, as well as specific evaluations and design feedback for the ICNIA designs.

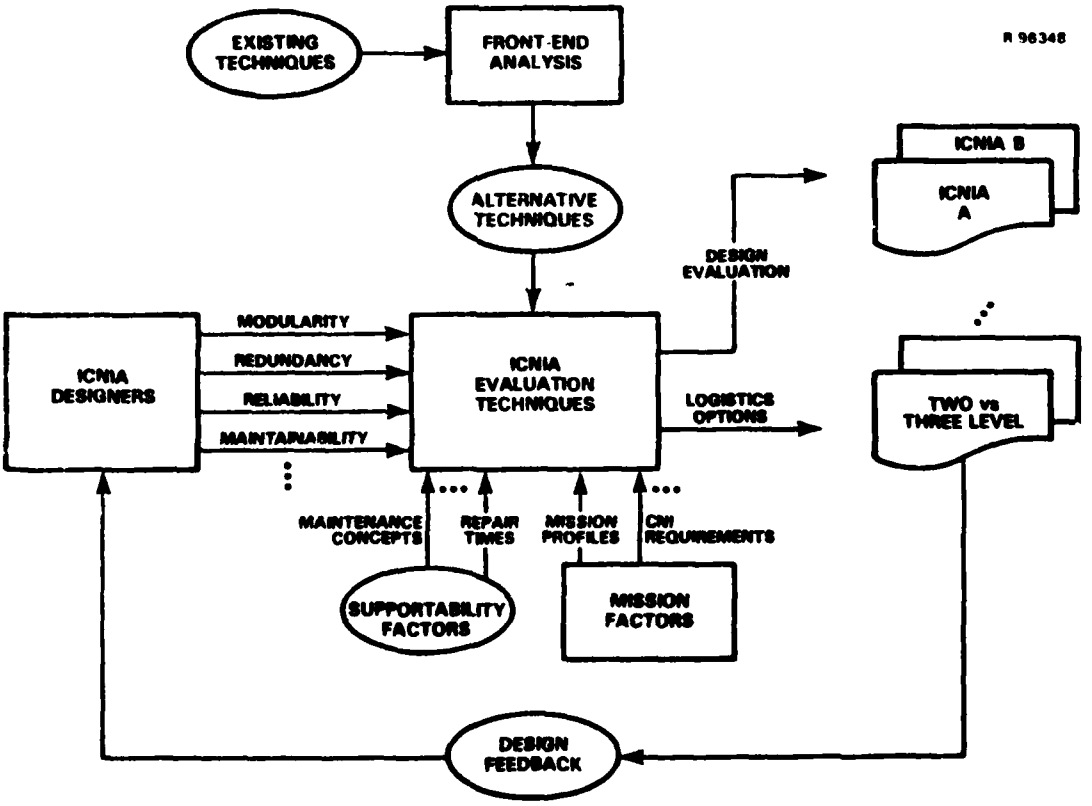


Figure 1. Overview of Impact Analysis of ICNIA

1.3 ORGANIZATION OF THIS PAPER

The Impact Analysis of ICNIA program is concerned with three major factors: reliability, logistics support and survivability. The methodology in each area draws on a common representation of the system. The reliability methodology is presented in Section 2. The system architecture representation, which is relevant to all three areas, is introduced, and an example is presented and analyzed extensively. Section 3 presents the logistics support analysis methodology. The same example is analyzed for supportability. Interim conclusions and recommendations are stated in Section 4.

Application of these methodologies to ICNIA Systems A and B will be reported in References 3 and 4, respectively. Design feedback for the architectures will be provided in these reports.

2. RELIABILITY ANALYSIS

The fault tolerance of ICNIA, achieved through dynamic reconfigurability, makes the analysis of system reliability more complex than for traditional systems. The integration of many radio functions creates interdependent failure modes that are not well described by existing measures of reliability. As a result, new measures of effectiveness are needed.

The applicability of previous work is examined in Section 2.1. A reliability methodology is then presented that includes development of fault tolerance indices and identification/classification of failure modes in a mission scenario. Mission scenarios are discussed in Section 2.3. An example architecture is presented in Section 2.4 and analyzed in Section 2.5. Some conclusions are drawn in Section 2.6.

2.1 FRONT-END STUDY FINDINGS

A front-end study was conducted to ascertain the applicability of existing reliability analysis techniques to ICNIA-type systems. The primary focus was to review the features of reliability models and procedures currently in use by the military services. Following is a brief summary of the techniques surveyed.

MIL-HDBK-217D Reliability Prediction of Electronic Equipment

This handbook is used for reliability estimation of individual components. Failure rates are estimated based on parts count and a stress analysis. While this procedure is applicable to individual components, it does not address system structure, which is the key to fault tolerance.

MIL-STD-756 Reliability Prediction

This standard is used for system reliability prediction. Conventional combinatoric probability is used to relate series/parallel structures to mission, or system, reliability. The reconfigurable aspect of ICNIA-type systems is not captured.

DEPEND

The Determination of Equipment Performance and Expected Nonoperational Delay (DEPEND) (Reference 5) models

reliability and availability for redundant systems with back-up modes of operation. The model considers the fault tolerance achieved through redundancy but not through the sharing of resources in an integrated system. As a result, the analysis of dynamically reconfigurable systems is limited.

AEP

The Avionics Evaluation Program (AEP) (Reference 6) estimates mission success and abort rates, as well as costs. The model is essentially a Monte Carlo simulation of flight operations in a specified scenario. Redundancy is modeled at the subsystem level. Component redundancy, integrated systems and dynamic reconfiguration are not addressed. In addition, the magnitude of the model makes it inappropriate as an interactive design tool.

None of the models reviewed appear adequate in the area of representing integrated, reconfigurable systems. The literature on reliability theory of complex systems was also reviewed. The framework of structural reliability as developed algebraically by Birnbaum, et al. (Reference 7), or the equivalent fault-tree approach (Reference 8), applies to these systems. However, existing computational techniques, such as those in Reference 9, seem inadequate for dealing with the complex system structures needed to realistically model the ICNIA systems.

One approach which has been taken to avoid the computational limits on reliability structures is Monte Carlo analysis. Even this approach requires the mapping from point failures into system failure. No suitable approach to defining this mapping for detailed ICNIA-type systems is available. Some progress in this area has been made by the ICNIA System A and B contractors. In particular, construction of the mapping has been avoided by the System B contractor by building a Monte Carlo simulation around the system control algorithm, which would determine whether a system failure occurred for each point failure that occurred. However, this approach does not lend itself to use as a reliability design tool in the early phases of development. The need for detailed data concerning the dynamic operating environment and the system controller, coupled with high computer run times, makes such a model cumbersome to use.

The primary conclusion of the front-end study was that the existing reliability techniques did not satisfy all of the analysis requirements for ICNIA-type systems. As a consequence, an essentially new methodology was developed and is described below.

2.2 METHODOLOGY

This section introduces the methodology for analyzing reliability of integrated, fault-tolerant systems. First, measures of effectiveness are defined. Next, a method of representing such systems by a structural reliability model is presented. Finally, computational techniques for the structural reliability model are developed. An overview of the model is provided at the end of the section.

Measures of Mission Reliability

Because of the multiplicity of functions supported by ICNIA and their varying importance to different missions, a combined measure of effectiveness for mission reliability is needed. We define Mission Completion Success Probability (MCSP) as the probability that a given set of critical functions is available throughout a given mission. A related measure is Mean Time Between Critical Failure (MTBCF), where a critical failure is a failure or a combination of failures that make a critical function unavailable. These measures are meaningful in a mission context where a set of CNI functions are considered critical for mission success. It is assumed that no repair action is taken between critical failures. When a single function is being considered as critical, MTBCF will be referred to as Mean Time Between Function Failure (MTBFF). Thus, the two measures are interchangeable when only a single function of the complete set of CNI functions is considered critical. A useful index of fault tolerance is failure resiliency, defined as the ratio of MTBCF (or MTBFF) to the traditional Mean Time Between Failure (MTBF). Since MTBF refers to the first failure in the system, failure resiliency is greater than or equal to one. Larger failure resiliency values correspond to systems with a higher degree of fault tolerance.

A single function is considered available if the system controller can select a configuration to bring the function up, with a specified level of performance. The availability of a set of functions is complicated by the competition between functions for resources. System resources are modeled as discrete "failure units" or components. A component fails as a unit and is monitored individually by the system controller for reconfiguration purposes. Component requirements vary over time depending on the presence of a signal or pilot input. The time history of component utilization can also be scheduled by the controller within certain tolerances. Thus, dynamic reconfigurability makes it difficult to determine whether functions conflict.

Structural Reliability Formulation

A practical approach to determining function availability is to classify components based on their dynamic features and then represent them accordingly in a static model structure. This approach makes rapid reliability computations possible and is taken in this study.

Three types of component utilization have been identified:

1. Contending: The functions are available if there is a configuration in which separate components are used to perform each function.

2. Timesharing: Each function utilizes a component a fraction of the time. A set of functions is available if there is a configuration in which no component is overloaded.

3. Noncontending: The functions are available if there are sufficient components for each individual function.

Components are contending with respect to certain functions if the components must be dedicated constantly, or at rigidly scheduled times, to supporting the functions (e.g., receivers used to monitor communication channels). Components are timeshared if they are utilized by a function at flexibly scheduled times so that several functions can be interleaved (e.g., data processors). Resources that can be used by any number of functions simultaneously, such as power supplies, are always noncontending.

The classification of components as contending, noncontending, or timesharing also depends on the times during a mission at which each function is required. If functions are not required simultaneously, all components are noncontending.

Within the context of these definitions, dynamic reconfigurability can be represented by a structural model which gives meaningful measures of reliability for a specific mission type. The mission is characterized by the functions required and the simultaneity of these functions.

Structural Reliability Computations

In order to compute MCSP for a given mission scenario with specified function requirements, the mapping from system health (the state of each component) to functional capability is needed. Unfortunately, traditional approaches to evaluating this mapping (Reference 9) are practical only for systems with a certain modular structure that does not apply to ICNIA architectures. Furthermore, it is desirable to represent this mapping for individual functions rather than complete missions, so that a variety of missions can be constructed from a single data base.

For the ICNIA architectures that have been examined, it is possible to take advantage of the special structure of this mapping to compute MCSP efficiently. The computations, as implemented in the MIssion REliability Model (MIREM), are detailed in Appendix A. The basic approach is to assume a structure corresponding to two levels of reconfigurability or switching. This type of structure is illustrated in Figure 2.

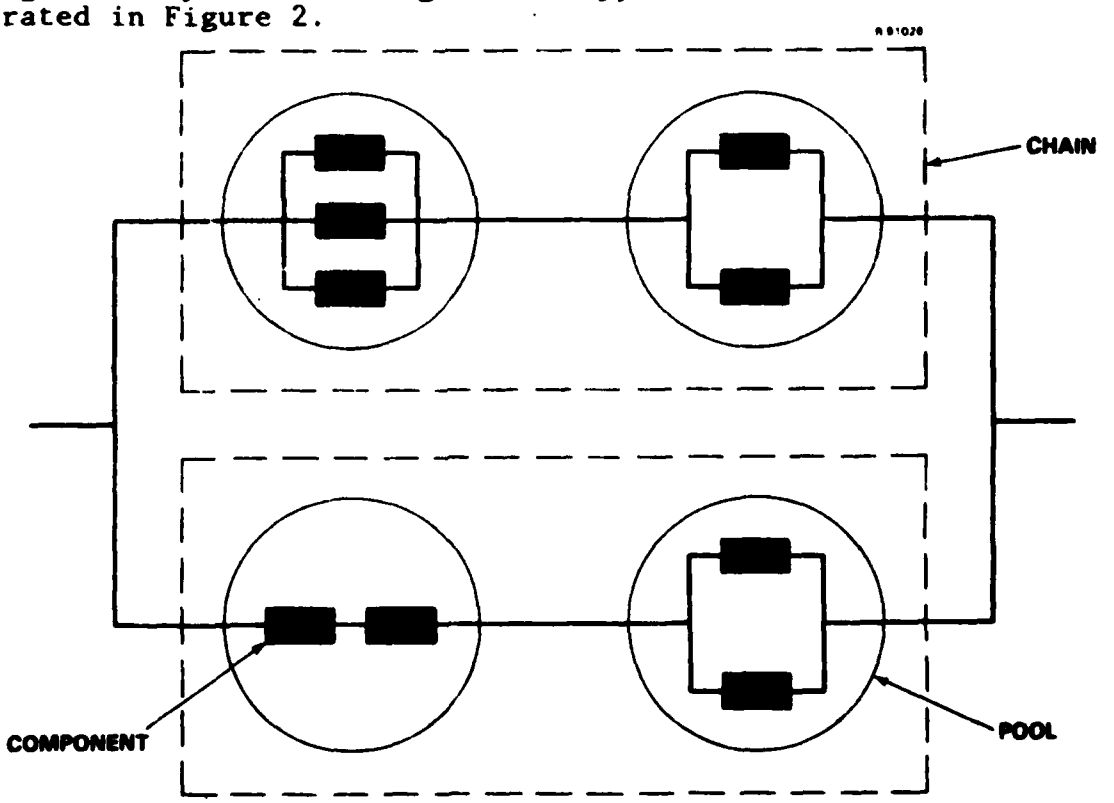


Figure 2. A Two-Level Structure for System Architecture Representation

At the lowest level, pools of interchangeable components are identified. Each function utilizes a certain number of components (or fraction of a component) in a pool. For pools of contending or timeshared components, the total requirement for a pool is the sum of the utilizations of each required function; for noncontending components, the total requirement is the maximum function utilization. If functions are not required simultaneously, all pools are considered noncontending. MCSP is the product of the probabilities of each pool having sufficient components operating.

The second level of reconfiguration is between parallel chains. A chain is a set of pools that is switched (reconfigured) as a group. In many cases a chain will correspond to a Line Replaceable Unit (LRU), because they have separate power supplies and limited inter-LRU connections. A set of functions is available on parallel chains if there is an allocation of functions to chains such that each chain can support its allocated functions. The approach to evaluating MCSP on parallel chains consists of enumerating all possible allocations of functions to chains (see Appendix A). This approach is computationally feasible whereas the traditional enumeration of component states is not, the difference being that there are many more components than required functions.

Total system MCSP is the product of the MCSP for each chain/parallel chain set. Other measures of effectiveness can be derived from MCSP. Of particular importance are MTBCF, which is computed by evaluating and numerically integrating MCSP for different mission durations, and failure resiliency, which is defined as the ratio of MTBCF to MTBF.

The reliability analysis methodology is summarized in Figure 3. System structure data are converted to files containing the pool and chain data needed by MIREM. With the additional inputs of failure rates, mission requirements and initial system health, MIREM computes measures of effectiveness plus LRU failure probabilities for use in the logistics analysis.

2.3 MISSION SCENARIOS

A mission can be described by a time sequence of CNI radio system or function requirements. Several factors affect whether the operational requirements of a mission can be met in a given state of system health:

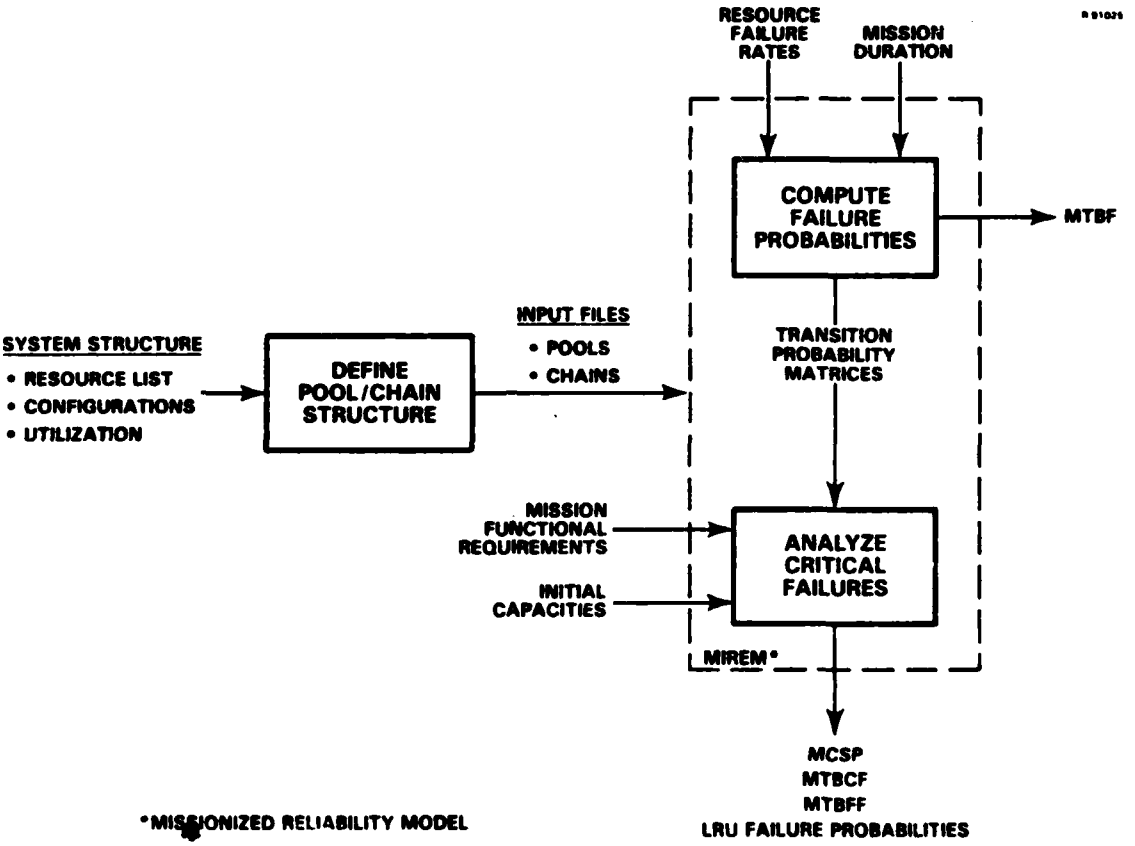


Figure 3. Reliability Analysis Overview

1. The set of critical functions (CF) required for the mission.

2. The combinations of these functions that are required simultaneously.

3. The time slots during which resources must be used to process signals within the interval when a function is required.

4. The time response required when a function requirement is received compared with the reconfiguration speed of the system.

The last two factors can generally be modeled by appropriate classification of pools as contending or noncontending, and selection of pool capacity requirements. The

first two factors have been dealt with in previous efforts (Reference 10) by dividing the mission into phases, each of which has distinct function requirements. In the current analysis, a single set of functions is considered for two cases of simultaneity:

(a) All functions are required simultaneously.

(b) Each function is required independently.

These two cases bound the actual mission environment. The worst case, (a), is used as the baseline for analysis.

The current analysis could be generalized to consider mission phases by including logical "or"s in the function requirements; e.g., (A and B) or (A and C and D). Although each phase would have a term in the logical expression, it could be reduced to a few dominant terms. In this manner, varying mission requirements could be analyzed with a static, structural model.

The mission scenarios which have been identified for analysis are listed in Table 1 (References 10, 11, and 12). These scenarios will be used to analyze the ICNIA systems A and B. Interdiction/Offensive Counter Air will be used as a baseline for analysis.

TABLE 1. MISSION REQUIREMENTS

SCENARIO	CRITICAL FUNCTIONS
Interdiction/Offensive Counter Air	UHF, JTIDS, GPS, IFFT
Close Air Support	HF, VHF, UHF, SEEK TALK, SINCGARS, JTIDS, IFFT
Defensive Counter Air	UHF, VHF, SEEK TALK, IFFI, IFFT
"Generic"	ILS, UHF, A/J VOICE, GPS, TACAN, IFFT
"Most Stringent" Simultaneous Requirements	HF, VHF, VHF (GUARD), UHF, UHF (GUARD), JTIDS, IFFT, IFFI

The functions listed for these scenarios are those necessary for survival/safety and mission success. Alternative requirements keyed only to survival could also be used to assess the impact of the system on aircraft losses.

2.4 APPLICATION TO AN EXAMPLE ARCHITECTURE

A simple example of a fault-tolerant architecture is discussed here to illustrate MIREM capabilities. The structure is shown in Figure 4. Low-band functions require one of the two low-band receive front ends; hence, they form the pool B. Low-band functions also require preprocessors in the set C or D. The UHF and SINCGARS functions, for example, require a total of two of the five preprocessors. Preprocessors in set C can be used only if certain other components in the larger group II are up. Similarly, the set D depends on components in group III.

This two-level structure is typical of those found in ICNIA designs (References 13 and 14). MIREM classifies C and D as pools and II and III as parallel chains. Pools A and B can be considered a series chain. Connection between these parallel chains is through the series chain (1). Pool boundaries are defined by the first level of reconfigurability; parallel chains are defined by the second.

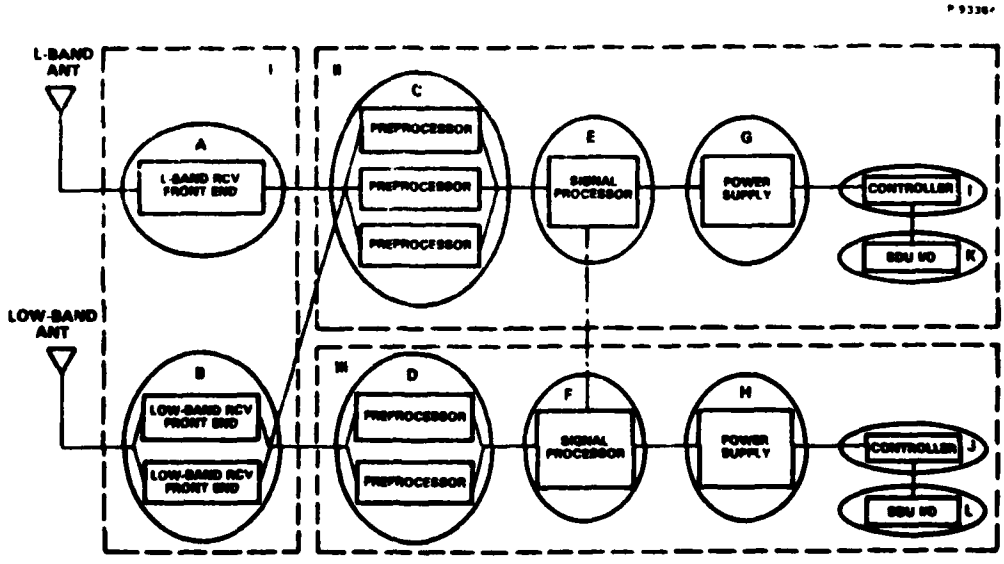


Figure 4. A Simplified Fault-Tolerant Architecture (CNI Receive Functions)

The input data required by MIREM for each pool are shown in Table 2. The table indicates that GPS, for example, requires one L-band receiver front end, three preprocessors, 80% of the capacity of a signal processor, one power supply, and one controller. The manner in which functions interact is given under pool type. Timesharing and contending pools are listed as type C; noncontending pools are listed as type N. Pool type dictates how utilizations are combined across functions. For example, the combination of UHF and SINCGARS requires two preprocessors but only one front end. Table 2 also shows the number of components, or capacity, and the component failure rate in each pool. Components within a pool are assumed to be identical.

Two other pool types are also considered. A set of pools, one in each parallel chain, is shared (type S) if the pool in one chain can be used by functions allocated to another chain. Chain-fail pools (type F) are those which, upon failure, prevent any of the pools in the chain from being utilized. In this example the signal processors are connected by a data bus, so that they are shared by chains II and III. Loss of a power supply prevents any of the pools in that chain from being used.

Many reconfigurable designs can be modeled by the pool/chain concept. However, care must be taken to represent failure modes properly, particularly for switching and control resources. The interpretation of backup components as a pool, i.e., components that are in parallel, assumes that the backup will take over when a component fails. This is accomplished in ICNIA through Built-In Test (BIT) equipment, RF switching and flexible processor interconnections, all coordinated by a control processor. Failures in these components can be modeled as an additional pool. The fact that not all failures can be detected by BIT, however, is not modeled.

2.5 RESULTS

Reliability results are presented in this section for the example introduced in Section 2.4. Table 3 shows MTBFF and failure resiliency for each function considered individually and independent of any mission. UHF and SINCGARS both have very good reliability. This is explained by the fact that no single component failure can make these functions unavailable. GPS, being restricted to chain II, has several critical components, thus it exhibits a low MTBFF. The fault

TABLE 2. MIREM INPUT DATA

POOL	CHAIN	DESCRIPTION	UTILIZATION (NO. OF COMPONENTS)			CAPACITY (NO. OF COMPONENTS)	COMPONENT FAILURES PER 10^6 HRS	POOL TYPE
			GPS	UHF	SINC GARS			
A	I	L-Band Receiver Front End	1	-	-	1	100	N
B	I	Low-Band Receiver Front End	-	1	1	2	200	N
C D	II III	Preprocessor	3	1	1	3 2	600	C
E F	II III	Signal Processor	0.8	0.1	0.4	1 1	200	S
G H	II III	Power Supply	1	1	1	1 1	40	F
I J	II III	Secure Data Unit I/O	-	-	1	1 1	40	N
K L	II III	Controller	1	1	1 1	1	200	N

TABLE 3. FUNCTION RELIABILITY

FUNCTION	MTBFF (hrs)	FAILURE* RESILIENCY
GPS	467	2.08
UHF	2126	9.48
SINCGARS	2042	9.11

*FAILURE RESILIENCY = MTBFF/MTBF;
MTBF = 224 hours

tolerance is best seen in the failure resiliency, which roughly corresponds to the number of failures that occur before a function failure.

System reliability in a mission context, expressed by MTBCF, is considerably lower. Two mission scenarios are considered in Table 4, one requiring all three functions simultaneously, and one requiring only UHF and SINCGARS. Both missions are three hours in length. For Scenario 1, fault tolerance only extends the MTBF of 224 hours to a MTBCF of 249 hours, whereas for Scenario 2 the increase is dramatic. Hence, failure resiliency is very dependent on the mission scenario. Only 2.5% of the critical failures for Scenario 1 occur in chain I, with the rest occurring in the parallel chains II and III. If the functions are not required simultaneously, the MTBCF for Scenario 1 increases to 389 hours, with a failure resiliency of 1.74.

TABLE 4. MISSION RELIABILITY

MISSION SCENARIO	MCSP (3-hour mission)	MTBCF (hours)	FAILURE* RESILIENCY
1 GPS, UHF AND SINCGARS required simultaneously	0.9880	249	1.11
2 UHF and SINCGARS required simultaneously	0.999996	1379	6.15

*Failure Resiliency = MTBCF/MTBF; MTBF = 224 hours

A major advantage of MIREM as a design tool is its ability to evaluate the impact of proposed design changes. Table 5 shows the sensitivity of MCSP to redundancy levels using the architecture discussed above as the baseline. Adding a second signal processor to chain II, for example, reduces the probability of mission failure (1 - MCSP) by 10%. Additional preprocessors improve reliability dramatically because of their high failure rate and because all five are required for this scenario. Other mission scenarios would show different sensitivities.

Table 6 gives the sensitivity of MCSP to the degree of reconfigurability of the system. The primary restriction to reconfigurability is that GPS must use chain II. Adding the appropriate switching and a third preprocessor to chain III, so that GPS can use either chain, has a large reliability payoff. On the other hand, reducing reconfigurability by eliminating the data bus between the signal processors does not significantly degrade reliability.

TABLE 5. SENSITIVITY OF MCSP TO REDUNDANCY LEVELS FOR SCENARIO 1

REDUNDANCY OPTION		NEW* MCSP	% REDUCTION IN MISSION FAILURES
BASELINE ARCHITECTURE	PROPOSED MODIFICATION		
2 Signal Processors	3 Signal Processors (2 in chain II)	0.9892	10
5 Preprocessors (3 in chain II, 2 in chain III)	6 Preprocessors (4 in chain II)	0.9970	75
	6 Preprocessors (3 in chain III)	0.9916	30
1 L-band Receiver	2 L-band Receivers	0.9883	3

*Baseline MCSP = 0.9880

TABLE 6. SENSITIVITY OF MCSP TO RECONFIGURABILITY FOR SCENARIO 1

RECONFIGURABILITY OPTION		NEW* MCSP	% REDUCTION IN MISSION FAILURES
BASELINE ARCHITECTURE	PROPOSED MODIFICATION		
Share signal processors between chains	Separate signal processor for each chain	0.9880	0
GPS must use chain II	GPS can use chain II or III (add 3rd preprocessors to chain III)	0.9970	75

*Baseline MCSP = 0.9880

2.6 CONCLUSIONS

A structural reliability model has been presented which can represent the features of integration and fault tolerance in complex systems. The model focuses on dynamic reconfigurability and does not consider the issues of Built-In Test (BIT) coverage, software inadequacies or failures and cabling failures. Several conclusions can be drawn from the reliability example which was analyzed:

1. Single components that can cause system failures (critical failures), if they exist, are the single most important factor in Mission Completion Success Probability (MCSP) and a major factor in Mean Time Between Critical Failure (MTBCF).

2. A second level of redundancy (at the LRU level) improves reliability only if all critical functions are supported on both of the LRUs.

3. The determination of which functions are critical for a mission and whether they are required simultaneously can drastically affect MCSP.

4. Reconfigurability (e.g., inter-LRU connections) between components that are already redundant do not necessarily enhance reliability.

Efficient computation of reliability measures is possible with this model. Furthermore, the model has the advantage of not requiring highly detailed design inputs.

3. LOGISTICS SUPPORT ANALYSIS

The potential advantages of integrated, fault-tolerant CNI avionics from the logistics support perspective are readily apparent. Some of the larger impacts are expected in:

1. Adoption of two-level maintenance.
2. Faster turnaround at the flight-line level.
3. Greater number of sorties between corrective maintenance actions.

These changes offer payoffs in both Life-Cycle Cost (LCC) and operational readiness. Integrated, fault-tolerant architectures exhibit the potential for increasing readiness levels above those of existing discrete systems at equal or lower LCC. This feature has added meaning with the emerging requirements of sustained combat capability under a bare base (i.e., no repair capability) environment with limited spares budgets. To achieve this objective, however, emphasis needs to be placed not only on hardware/software reliability and system architecture, but also on Built-In Test (BIT), modularity, and support strategies.

This section presents a method of evaluating the operational readiness payoff of integrated, fault-tolerant avionics. The method can evaluate alternative repair strategies and is consistent with the limited data available during the early stages of system design. An overview of the methodology is shown in Figure 5. The applicability of previous work is discussed in Section 3.1. The logistics support scenario to be modeled is described in Section 3.2. Section 3.3 presents the modeling methodology. Model inputs for an example architecture are defined in Section 3.4, and results are given in Section 3.5. Some conclusions are drawn in Section 3.6.

3.1 FRONT-END STUDY FINDINGS

Several logistics analysis techniques were assessed as to applicability to analysis of integrated, fault-tolerant architectures using both conventional and innovative maintenance concepts. In particular, six models were evaluated in some depth. Brief discussions of these six models, their

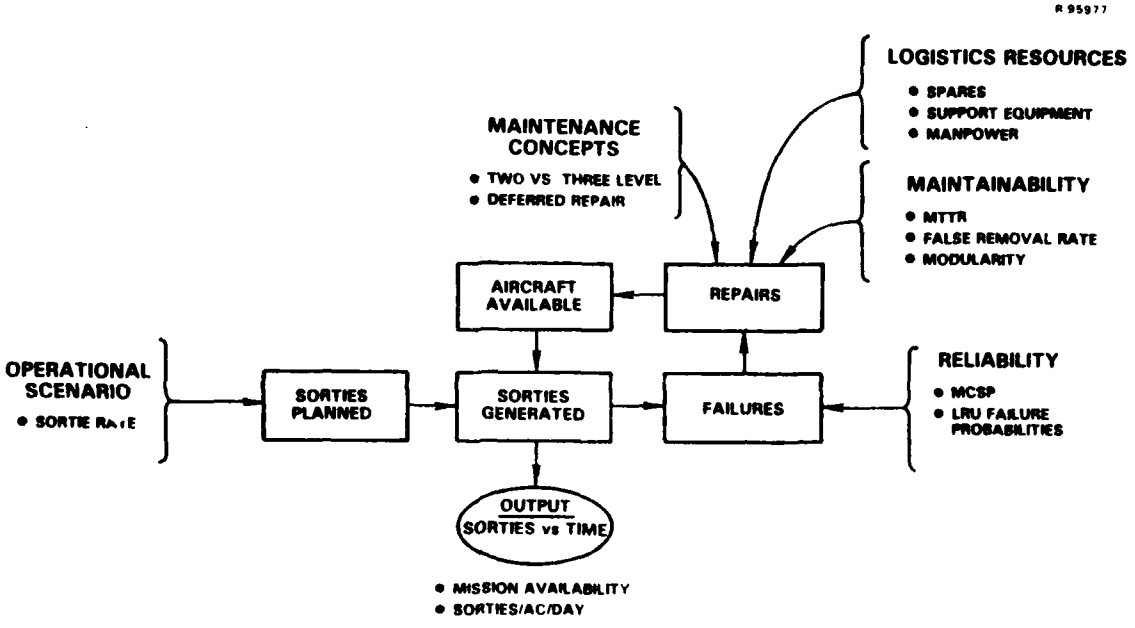


Figure 5. Readiness Methodology Overview

principal features and applicability to the ICNIA analysis requirements are provided in the following paragraphs.

ALPOS - The Avionics Laboratory Predictive Operations and Support model (Reference 15) is a parametric operating and support cost model based on historical data. It was derived using multiple regression techniques. It does not capture the integrated fault-tolerant characteristics of ICNIA nor can it model the innovative maintenance concepts applicable to ICNIA.

LCOM - The Logistics Composite Model (Reference 16) is a discrete event simulation model based on Monte Carlo techniques which captures in very fine detail the logistics structure of the maintenance scenario and the hardware structure (typically of a major weapon system). It does not lend itself to early design work, where the data are limited, although it could be streamlined with some effort.

ORLA - Optimum Repair Level Analysis (Reference 17) is an expected value model for determining optimum (least cost) policies for repairing/discarding LRUs and/or Shop

Replaceable Units (SRUs) at the intermediate or depot level. Determinations are based on spares, support equipment, and other support costs. The technique does not capture the fault-tolerant characteristics of ICNIA since it is driven largely by MTBF and traditional support factors.

LSC - The Logistics Support Cost (Reference 18) model consists of 10 equations which address support costs. The model does not explicitly capture innovative maintenance concepts applicable to ICNIA.

LCC2 - The Life-Cycle Cost Model Version 2 (Reference 19) is based on LSC equations. Although it provides flexibility as to maintenance concept modeling, it does not capture readiness factors and is not applicable to the early design phase.

MOD-METRIC - The MOD-METRIC model (Reference 20) is a set of sparing algorithms that treats the multi-item, multi-echelon, and multi-indenture inventory problem in an optimization framework. The model is limited to spares and does not capture the relevant logistics factors impacting system readiness.

Dyna-METRIC - The Dyna-METRIC model (Reference 21) incorporates dynamic queueing equations that extend the MOD-METRIC capabilities to transient behavior under time-varying operations. Like MOD-METRIC, the model addresses optimal sparing and spares availability, but does not capture other logistics factors impacting system readiness.

SOAR - The Simulation of Operational Availability/Readiness model (Reference 22) is a continuous flow simulation model based on system dynamics techniques that capture the reliability and maintainability parameters of a system with the dynamics of logistics support at a single base in order to evaluate mission availability at the squadron or wing level. It is applicable to early system design and its network flow framework can be extended to capture innovative maintenance concepts for ICNIA.

The main conclusion drawn from this front-end study is that no single technique captures all of the ICNIA analysis requirements. These models were developed with specific objectives in mind and address some of the ICNIA analysis needs but not all. The SOAR model appeared to be the technique closest to the ICNIA logistics support analysis requirements. This technique was selected for analysis of operational readiness with some modification for capturing innovative maintenance concepts.

3.2 LOGISTICS SUPPORT SCENARIO

The logistics support scenario being modeled incorporates the dynamics of aircraft sortie and maintenance operations at a single site (e.g., air base) from the perspective of the equipment under study (Figure 6). Weapon system sortie requirements, expressed in terms of desired number of sorties per day, are generated over a given time period. The weapon system is viewed in terms of the equipment under study and the rest of the aircraft with their associated reliability and maintainability parameters and support resources. Maintenance operations and logistics support at the organizational, intermediate and depot level maintenance sites are represented.

The flight line, or organizational-level, maintenance activities consist primarily of removal and replacement (R/R) of Line Replaceable Units (LRUs). For fault-tolerant system applications, R/R actions may take place when the first failure occurs or be deferred until system critical failures occur (i.e., loss of a critical function). These two repair policies will be referred to as immediate and deferred repair, respectively. Deferred repair is an innovative maintenance concept which would require significant institutional changes to implement. The procedure would rely heavily on BIT equipment to determine system health and an intelligent system to make the repair/defer decision based on system health and the type of mission to be flown. Compromise maintenance policies, which would defer repair of some noncritical failures and repair others, could be developed based on the increased risk of additional failures causing a critical failure in a degraded system. For the mission scenarios and system architectures considered to date, however, the increase in risk is generally small.

After flight line removal, faulty LRUs then enter the intermediate, or I-level, maintenance shop under a three-level maintenance policy where they are repaired by R/R of the faulty SRUs. If a two-level maintenance policy is considered, then the LRUs are sent directly to the depot for repair. The depot activities consist of repair of the faulty LRUs or SRUs, depending on the maintenance concept.

The maintenance resources available at each level depend on the type of base at which operations are being modeled. Two scenarios have been identified. These scenarios will be used in the analysis of the ICNIA systems A and B in References 3 and 4, respectively.

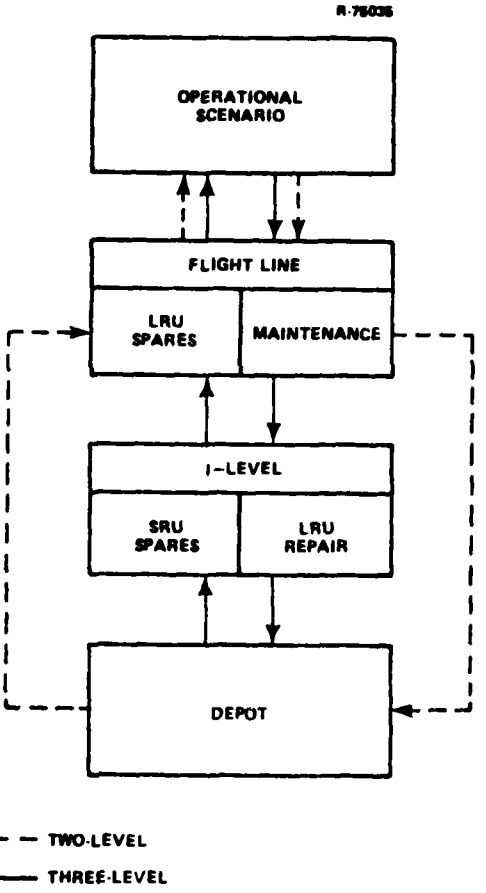


Figure 6. Logistics Support Scenario

Conventional Support Scenario

This scenario is representative of a fixed-site main operating base. The following maintenance resources are available for a squadron of 24 aircraft and systems:

1. Initial spares levels set at one spare for each LRU.

2. I-level shop for LRU repair, including one Automatic Test Equipment (ATE) work station available 12 hours each day and sufficient manpower.

3. Depot replenishment for SRUs (three-level maintenance) or LRUs (two-level maintenance).

An F-16 sortie schedule and an immediate repair policy are used as a baseline for this scenario. This 60 day schedule consists of a seven day surge or wartime sortie rate, a sustaining rate for days eight to 30 and a peacetime sortie rate of 0.7 sortie/aircraft/day for the last 30 days. Immediate repair is a reasonable baseline assumption for this scenario, since maintenance resources are not unduly stressed.

Advanced Support Scenario

This scenario represents a dispersed operating location, known as a bare base or austere site, and is consistent with the Air Force 2000 report. The following maintenance resources are available for a squadron of 24 aircraft and systems:

1. Initial spares levels set at one spare for each LRU.

2. An Industrial Maintenance Facility, which possesses depot repair capabilities, co-located with a Main Operating Base ("Queen Bee" base).

3. Depot SRU/LRU replenishment available only after the initial 7-day surge.

A maximum sortie schedule is used as a baseline for this scenario, putting maximum stress on the maintenance resources. Under this schedule, each ICNIA-equipped aircraft is launched as soon as it becomes available after rearm/refuel or repair. Deferred repair has the potential for sustaining more sorties in this limited-resource scenario, and is used as a baseline.

3.3 METHODOLOGY

Perhaps the most operationally significant dimension of logistics support, and one that is meaningful early in the development cycle, is readiness. For fighter aircraft, readiness can be viewed as the ability to satisfy an immediate or short-term requirement for sorties. To evaluate the operational readiness payoffs of integrated, fault-tolerant CNI systems, a logistics model that captures these issues and is consistent with existing data during the early stages of system design is needed. The Analytic Sciences Corporation (TASC) has developed the Simulation of Operational Availability/Readiness (SOAR) model to study readiness issues for advanced avionics systems (Reference 23).

SOAR has previously been applied to avionics systems such as the AN/ALQ-131, Airborne Self-Protection Jammer (ASPJ) and Low-Altitude Navigation and Targeting, Infrared for Night (LANTIRN). It has now been extended to accommodate deferred repair policies applicable to integrated, fault-tolerant avionics.

SOAR analyzes the dynamics of aircraft sorties and maintenance operations at a single site that are described in the logistic scenarios of Section 3.2. A system of linear differential equations is established for the expected flow rates into and out of major system states. Aircraft, systems, LRUs and SRUs move through ready, failed, and under repair states. These equations are solved by Euler's single-step method, starting from specified initial conditions. Different system states and flow diagrams are used for the cases of immediate and deferred repair.

Immediate Repair

The basic SOAR flow diagram for immediate repair is shown in Figure 7. Sorties are generated to meet the planned sortie rate or until the available aircraft and systems are exhausted. The expected number of LRUs returning faulty are routed to a repair queue, are repaired, and finally are reissued. Additional repair states and delays for LRUs and SRUs that depend on the level of repair are not shown.

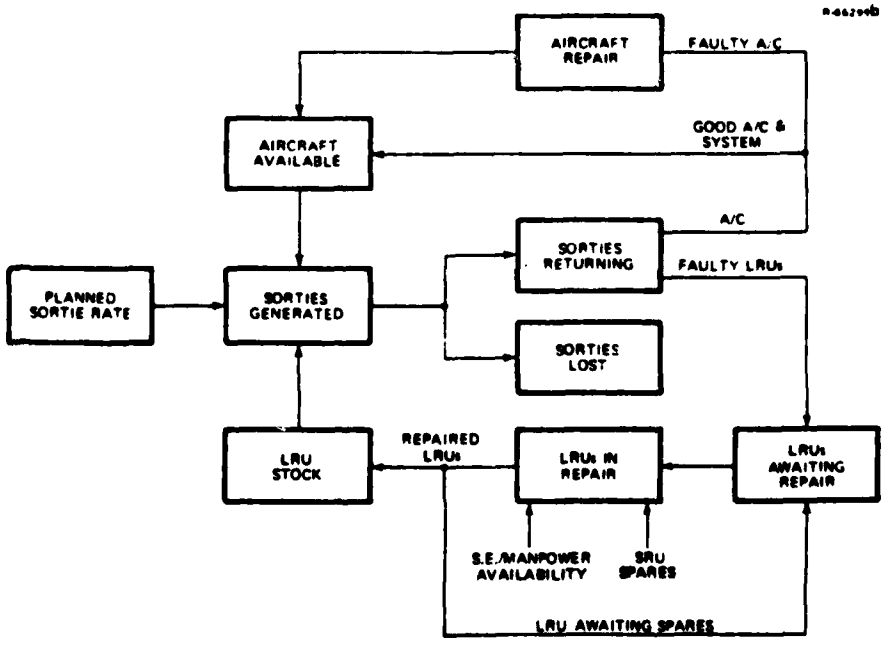


Figure 7. SOAR Avionics Model (Immediate Repair)

Deferred Repair

The SOAR flow diagram for deferred repair is shown in Figure 8. Unlike immediate repair, deferral of repair until a critical failure occurs results in a changing mission reliability. For highly fault-tolerant systems, reliability decreases as a system continues to be flown without repair. Hence, the age or operating time since repair of each system must be tracked by the model. Six categories of system age are counted as separate states in the model, with varying Mission Completion Success Probability (MCSP). Age also impacts which LRUs are pulled from systems returning faulty. On the average, more LRUs will be pulled from "old" systems.

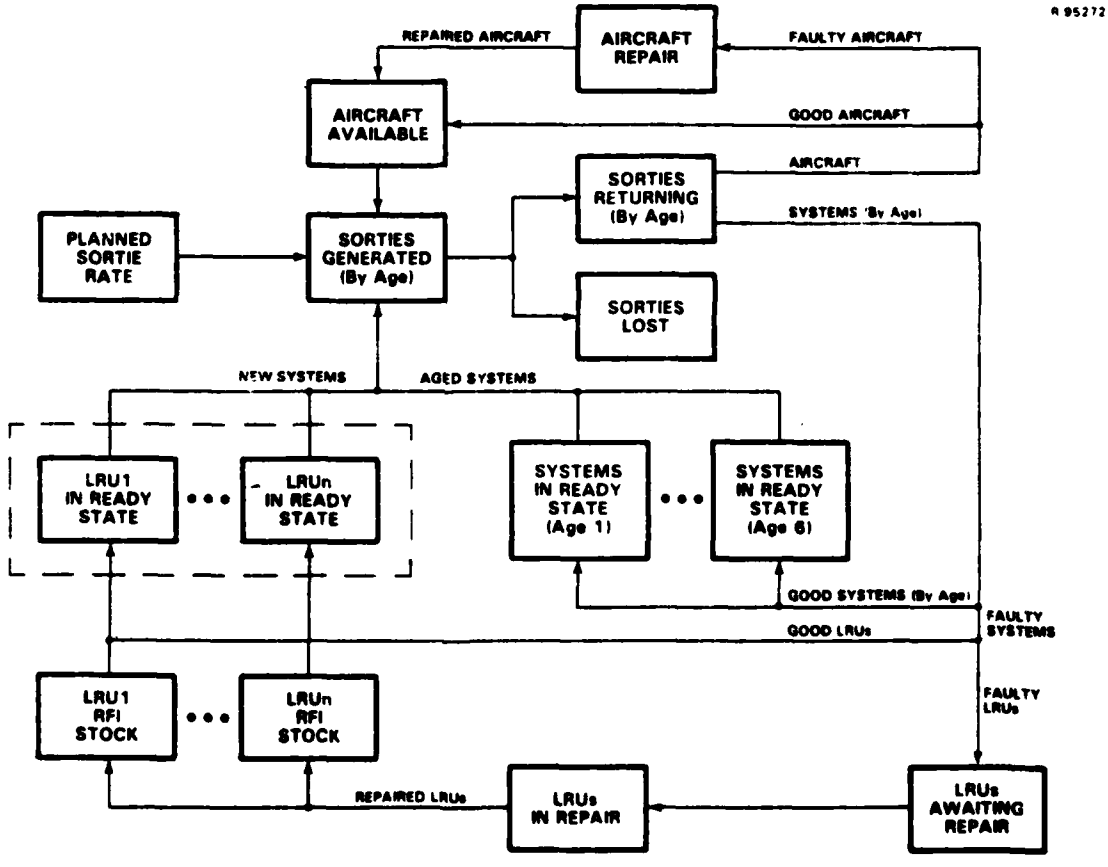


Figure 8. SOAR Deferred Repair Avionics Model

Once the faulty LRUs are pulled, the remaining LRUs return to "new" status. When they are combined with other Ready For Issue (RFI) stock, a new (age zero) system reenters the cycle. The remainder of the model is equivalent to the immediate repair model.

Measures of Effectiveness

The time sequence of any state variable or rate in the model can be obtained as an output from SOAR. Two primary measures of operational readiness have been identified as useful outputs:

(a) Mission Availability: The ratio of the actual number of sorties generated to the desired number.

(b) Sortie Generation Rate: The number of sorties generated per day per aircraft. The Primary Aircraft Authorization (PAA) is used as the number of aircraft; less aircraft may be available because of attrition. This measure is of interest when a maximum sortie generation schedule is being used.

3.4 MODEL INPUTS FOR AN EXAMPLE ARCHITECTURE

The inputs required by SOAR are listed in Tables 7 and 8. The values listed in these tables are for the baseline case reported in Section 3.5. Parameters that differ from these values for the conventional and advanced deployment scenarios are defined in Section 3.2. The architecture-dependent inputs are for the example architecture of Section 2.4. A three-LRU packaging is assumed, with one LRU for each chain as depicted in Figure 4.

The reliability inputs in Table 8 were generated by MIREM using the equations derived in Appendix A. The architecture of Section 2.4 and the mission requirements of Scenario 2 were used. These inputs pertain to deferred repair; conventional MTBF reliability measures are used as inputs for immediate repair. Each age interval in Table 8 corresponds to 100 hours of operation without repair. Note that for new systems an average of just over one LRU contains a failure when a repair action occurs, whereas for systems of age 6, two LRUs contain failures. In addition, the distribution of faulty LRUs shifts toward those with fault tolerance

TABLE 7. SOAR MODEL INPUTS

DESCRIPTION	NAME	VALUE
Mission Related		
Desired Sortie Rate (sorties/aircraft/day) — Surge	SX	*
Desired Sortie Rate (sorties/aircraft/day) — Intermediate	IX	*
Desired Sortie Rate (sorties/aircraft/day) — Peacetime	PX	0.7
Interval Between Sorties (hours)	SINTVL	1
Attrition Rate (fraction of sorties) — Surge	WARF	0
Attrition Rate (fraction of sorties) — Peacetime	PARF	0
Start of Surge Period (hours)	STWAR	0
End of Surge Period (hours)	ENDWAR	168
Start of Peacetime Period (hours)	STPEAC	720
Scenario Length (hours)	LENGTH	1440
Mission Length (hours)	ML	3
Aircraft Related		
Initial Number of Aircraft	INAC	24
Aircraft Returning Faulty (fraction)	DF	0
Turnaround Time for Faulty Aircraft (hours)	ATAT	9
Rearm/Refuel Time for Good Aircraft (hours)	FLDEL	2†
System Related		
Initial Number of (Age 1) Systems	PIRS1	24
LRU Turnaround Time at the I-Level Shop (hours)	MTAT	4
LRU False Removal Rate (fraction of LRU failures)	UFP	0.1
Support System Related		
I-Level Support Equipment and Manpower Availability (fraction of total time)	SAVAIL	0.5
Number of I-Level Testers	NSE	1
Number of Ready For Issue (RFI) Spares — LRU 1	RFI1	1
Number of Ready For Issue (RFI) Spares — LRU 2	RFI2	1
Number of Ready For Issue (RFI) Spares — LRU 3	RFI3	1
Base to Depot Shipping Time (hours)	BDST	360
Depot to Base Shipping Time (hours)	BRST	240

*Value is classified.

†A one hour rearm/refuel time applies to the conventional and advanced deployment scenarios defined in Section 3.2.

TABLE 8. SOAR RELIABILITY INPUTS (DEFERRED REPAIR)

LRU \ AGE*	1	2	3	4	5	6
PROBABILITY OF CRITICAL FAILURE DURING MISSION						
-	0.0001	0.0004	0.0007	0.0010	0.0013	0.0016
PROBABILITY THAT LRU IS FAULTY AT REPAIR						
1	0.11	0.15	0.19	0.22	0.26	0.29
2	0.92	0.94	0.95	0.96	0.97	0.98
3	0.26	0.40	0.50	0.57	0.63	0.68
EXPECTED NUMBER OF FAULTY LRUs	1.30	1.49	1.64	1.76	1.86	1.95

*Age of a system refers to the number of missions flown or hours of operation without undergoing repair. Six age ranges are established, each representing 100 hours or 33 missions.

(LRUs 2 and 3) as time since repair increases. The mission failure probability also increases with age. This increasing "failure rate" is due to the high fault tolerance of the architecture for this mission.

3.5 RESULTS

Readiness results are presented in this section for the architecture introduced in Section 2.4 and the logistics parameters listed in Section 3.4. A maximum sortie schedule and a high aircraft mission capable rate are used for this analysis to stress the maintenance resources. Figure 9 shows the sortie generation rate as a function of time for three-level and two-level maintenance concepts. With three-level maintenance, the spares and Intermediate-level shop throughput are sufficient to maintain maximum readiness. Thus, the system under study has no impact on aircraft availability. The maximum rate of 4.8 sorties/aircraft/day is determined by the five hour cycle of mission length plus rearm/refuel time.

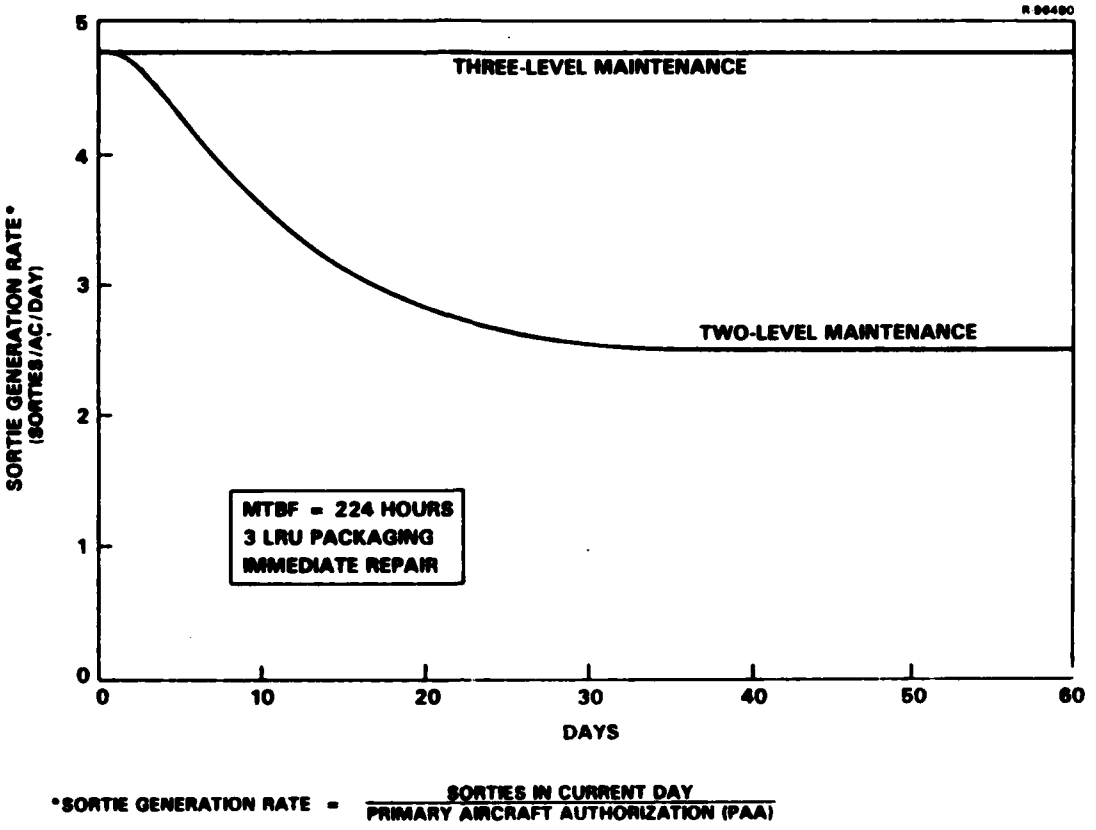


Figure 9. Maximum Sortie Generation by Level of Repair

Under two-level maintenance, readiness decreases as faulty LRUs are tied up in the longer repair pipeline and spares are exhausted. Equilibrium is reached at 2.3 sorties/aircraft/day when the LRU failures match the LRUs returning from depot.

Sortie generation rate can be increased under the two-level concept by providing more spares at the organizational level or by adopting a deferred repair policy. In Figure 10, immediate and deferred repair policies are compared under two-level maintenance. The deferred repair policy can sustain many more sorties than the immediate repair policy and nearly matches the sorties achieved under three-level maintenance. Even when the systems age and repair actions start to build up, the high MTBCF places less demand on the LRU repair pipeline and a higher sortie rate is maintained.

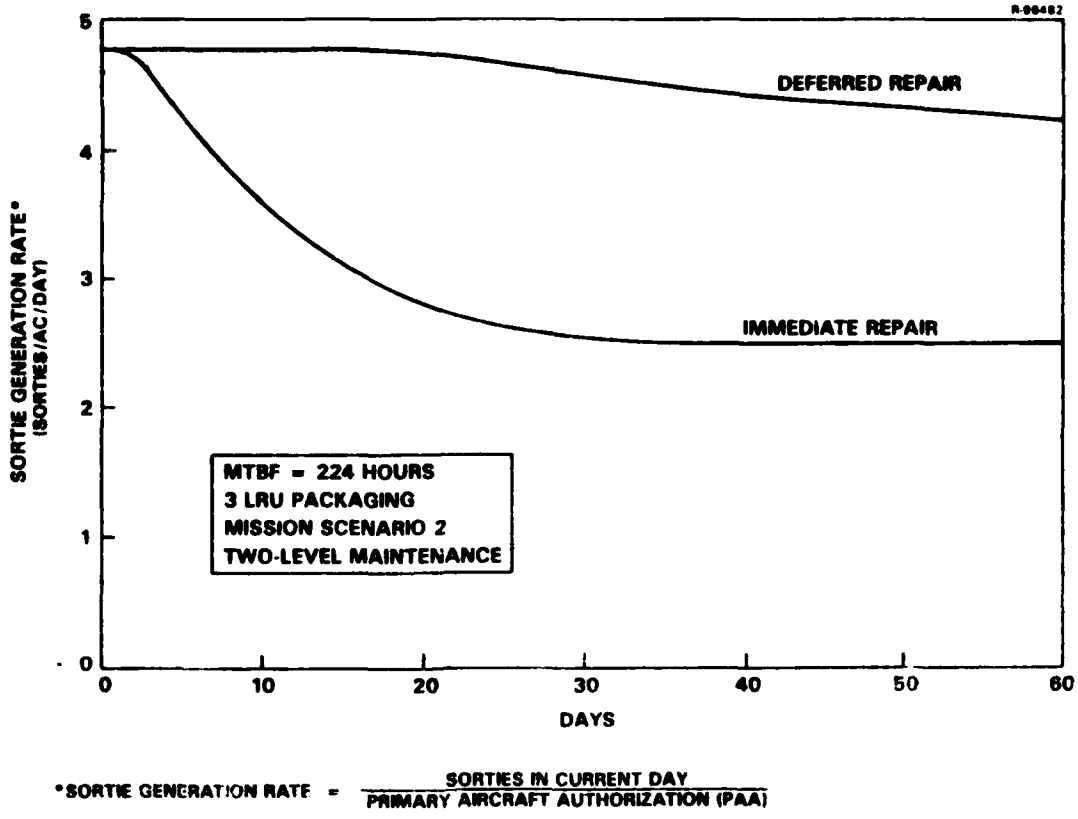


Figure 10. Maximum Sortie Generation by Repair Policy

A six-LRU packaging arrangement is compared with the baseline of three LRUs in Figure 11. Immediate repair is assumed so that only the traditional reliability inputs are required for the six LRUs. The six-LRU configuration (increased modularity) provides a higher system availability at the base and thus a higher sortie rate, since a smaller piece of the system is tied up in the repair pipeline for each failure.

The readiness benefits of three-level maintenance and increased modularity must be traded off against the associated increased costs. The readiness benefit of deferred maintenance, on the other hand, is really only traded against the slight increase in mission failure probability (assuming that BIT and resource managements features are already included for reasons of fault tolerance).

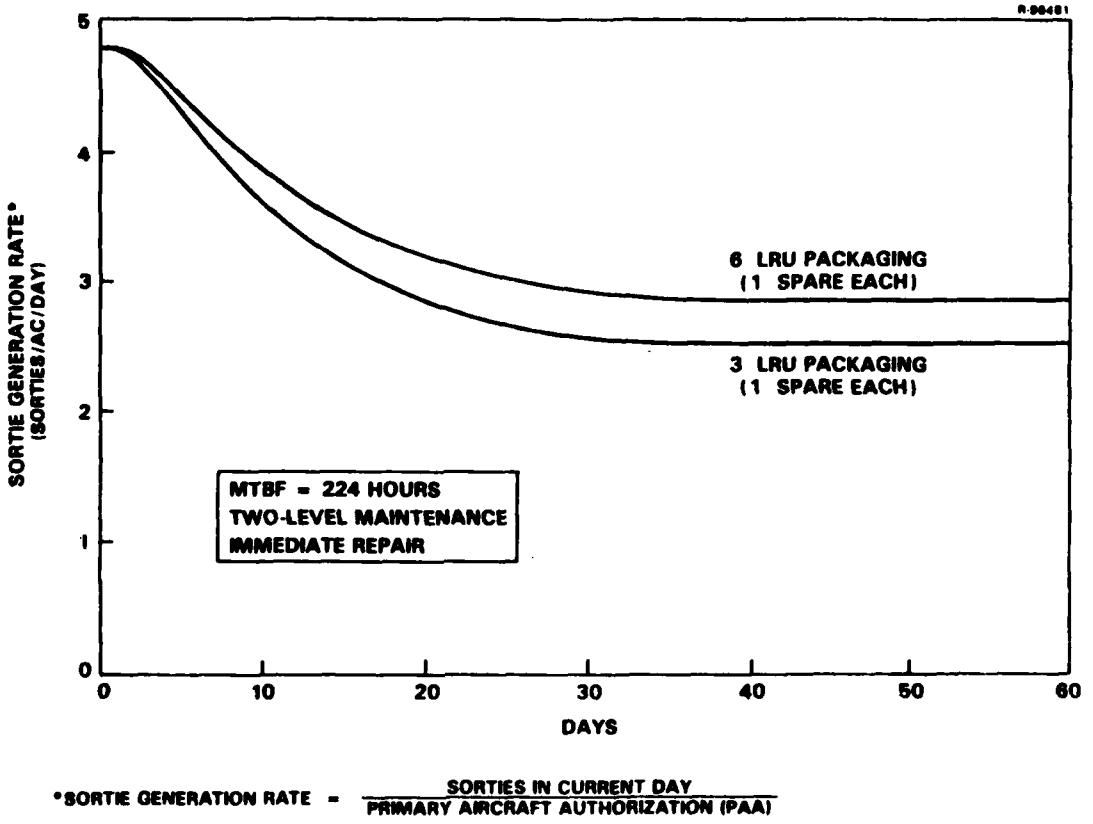


Figure 11. Maximum Sortie Generation by Modularity

3.6 CONCLUSIONS

A technique has been presented for assessing the readiness impact of integrated, fault-tolerant systems. The readiness impact of two- versus three-level maintenance, modularity and deferred repair have been illustrated. Two conclusions can be drawn from the supportability example which was analyzed:

1. Deferral of repair until a critical failure occurs allows a high sortie rate to be sustained for a longer period without repair. The payoff is substantial for highly fault-tolerant systems, particularly under a two-level maintenance policy. However, some penalty is paid in MCSP for flying systems that contain failed components (less redundancy).

2. High reliability, deferred repair policies and increased modularity all provide impetus to use two-level maintenance, eliminating expensive intermediate level test equipment.

This analysis technique is applicable to ICNIA architectures during the early stages of design. Specific sortie rate capabilities for ICNIA will depend on the system's reliability parameters.

4. INTERIM CONCLUSIONS AND RECOMMENDATIONS

A model has been presented which can represent the features of integration and fault tolerance in complex systems. Techniques for assessing the reliability and logistics support impacts of such an architecture were developed. These techniques are applicable to ICNIA architectures during the early stages of design. The reliability example illustrates the ability of the model to assess redundancy, reconfigurability and component quality in terms of mission reliability. The logistics support model demonstrated the readiness impact of two- versus three-level maintenance, deferral of repair actions until a critical failure occurs and modularity.

Several conclusions can be drawn from the example which was analyzed. For reliability,

1. Single components that can cause system failures (critical failures), if they exist, are the single most important factor in Mission Completion Success Probability (MCSP) and a major factor in Mean Time Between Critical Failure (MTBCF).

2. A second level of redundancy (at the LRU level) improves reliability only if all critical functions are supported on both of the LRUs.

3. The determination of which functions are critical for a mission and whether they are required simultaneously can drastically affect MCSP.

4. Reconfigurability (e.g., inter-LRU connections) between components that are already redundant does not necessarily enhance reliability.

In terms of supportability,

1. Deferral of repair until a critical failure occurs allows a high sortie rate to be sustained for a longer period without repair. The payoff is substantial for highly fault-tolerant systems, particularly under a two-level maintenance

policy. However, some penalty is paid in MCSP for flying systems that contain failed components (less redundancy).

2. High reliability, deferred repair policies and increased modularity all provide impetus to use two-level maintenance, eliminating expensive intermediate-level test equipment.

The techniques developed have the advantage of not requiring highly detailed design and logistics inputs and of being relatively streamlined. The computerized models are amenable to interactive use and could be hosted on a minicomputer. As a result, the techniques could be applied early in the design phase as a design tool to aid the engineer in building reliability and supportability into an integrated system.

Several areas of additional research are suggested by this study. The reliability model developed here does not include the effects of incomplete or faulty BIT coverage, which could cause incorrect switching by the system controller. For highly fault-tolerant systems, this effect is likely to be significant. Software reliability and fault tolerance, which will become increasingly important in these systems, also needs further research. Maintenance concepts that rely on smart systems to schedule and reduce the number of repair actions pose another major issue. The implications of attempting to institutionalize such a concept need to be explored. Finally, the enhancement and possibly integration of the models developed here into an interactive, user-friendly package is required if they are to be used by design engineers.

REFERENCES

1. Harris, R.L., "Future Directions in CNI Integrated Avionics," IEEE NAECON 81 Proceedings, May 19-21, 1981, pp. 338-344.

2. Camana, P.C., and Campbell, M.E., "Integrated CNI Avionics Maximizes Reliability," IEEE NAECON 82 Proceedings, May 18-20, 1982, pp. 42-45.

3. Veatch, M.H., "Impact Analysis of ICNIA System A," The Analytic Sciences Corporation, Technical Report TR-4128-2.

4. Veatch, M.H., "Impact Analysis of ICNIA System B," The Analytic Sciences Corporation, Technical Report TR-4128-3.

5. "KU-band Reliability Improvement -- User's Manual for TASA/DEPEND Program," Air Force Wright Aeronautical Laboratories, AFAL-TR-78-135, Vol. 3, September 1978.

6. "Avionics Evaluation Program: Multiple Aircraft, Multiple Sorties, and Cost Accumulation," Air Force Wright Aeronautical Laboratories, AFAL TR-76-196, January 1977.

7. Birnbaum, Z.W., Esary, J.D., and Saunders, S.C., "Multi-Component Systems and Structures and their Reliability," Technometrics, Vol. 3, 1961, pp. 55-77.

8. Barlow R.E., and Proschan, F., "Importance of System Components and Fault Tree Events," Stochastic Processes and Their Applications, Vol. 3, 1975, pp. 153-172.

9. Birnbaum, Z.W., and Esary, J.D., "Modules of Coherent Binary Systems," SIAM Journal, Vol. 13, 1965, pp. 444-462.

10. Long, W.S., "Mission Scenario/ICNIA Prioritization Development," General Dynamics presentation, January 19-20 1982.

11. "Preliminary Prime Item Development Specification for Integrated Communication Navigation Identification Avionics (ICNIA) Terminal," TRW Electronic Defense Sector, July 1982.

REFERENCES (Continued)

12. Conversations with ITT Avionics Division personnel, March 3, 1983.

13. "Integrated Communications, Navigation and Identification Avionics Project, Interim R&D Status Report," TRW Electronic Systems Group, March 1982.

14. "Integrated Communications, Navigation and Identification Avionics Systems Definition Study, Interim Technical Report," ITT Avionics Division, January 1982.

15. "The Avionics Laboratory Predictive Operations and Support (ALPOS) Cost Model," Air Force Wright Aeronautical Laboratories, AFAL TR-78-49, Vol. II, April 1978.

16. "Logistics Composite Model (LCOM) Simulation Software Users Reference Guide," Air Force Management Engineering Agency, AFMSMMET Report 81-1.1, March 1982.

17. "Optimum Repair Level Analysis (ORLA)," Air Force Logistics Center Manual, AFLCM-800-4.

18. "Logistics Support Cost Model User's Handbook," Air Force Logistics Center/Acquisition Logistics Division (AFLC/ALD), August 1976.

19. Gates, Robert K., et al., "Program LCC Documentation Version 2," The Analytic Sciences Corporation, Technical Report TR-747-3, April 1976.

20. "Recoverable Inventory Control Using MOD-METRIC," Headquarters, Air Force Logistics Center, AFLCP 57-13, February 1975.

21. Hillestad, R.J., "Dyna-METRIC: Dynamic Multi-Echelon Technique for Recoverable Item Control," The Rand Corporation, Report No. R-2785-AF, July 1982.

22. "Simulation of Operational Availability/Readiness (SOAR) Model Overview," The Analytic Sciences Corporation, Report No. EM-2194, October 1981.

23. Calvo, Alberto B., "Techniques for System Readiness Analysis," IEEE NAECON 82 Proceedings, May 1982, pp. 628-634.

REFERENCES (Continued)

24. Butler, D.A. and Lieberman, G.J., "Inspection Policies for Fault Location," Dept. of Statistics, Oregon State University, Technical Report 81, September 1982.

APPENDIX A
MISSION RELIABILITY MODEL (MIREM)

This appendix describes the equations and algorithms used in the MIssion REliability Model (MIREM). The model's basic function is to evaluate the combinations of failures which result in failure of a particular mission and compute the probability of such failures. Intrinsic hardware reliability is not predicted by the model, but treated as an input. The problem to be solved is defined in Section A.1 and the approach taken is presented in Section A.2. The reliability computations are developed in Sections A.3 and A.4. Finally, some additional model outputs are derived in Sections A.5 and A.6.

A.1 THE NETWORK RELIABILITY PROBLEM

We assume that the system consists of n components or "failure units" with constant failure rate. The traditional approach is to represent system health by $\underline{X}$, where X_i is equal to one if component i is up at the end of the mission and zero otherwise. For each mission M the system structure function (Reference 7)

$$\phi_M(\underline{X}) = \begin{cases} 1 \text{ if the mission M can be supported with system health } \underline{X} \\ 0 \text{ otherwise} \end{cases}$$

is determined and $\Pr\{\phi_M(\underline{X}) = 1\}$ is evaluated enumeratively. Unfortunately, this approach is practical only if the system has few components or can be decomposed into modules (Reference 9) of intermediate size. Furthermore, in order to analyze various mission requirements it is desirable to express ϕ at the individual function level rather than for a mission. Missions with various Communication, Navigation and Identification (CNI) function requirements can then be formulated if a "combining" operation is defined on the functional structures.

A.2 A SPECIAL STRUCTURE FOR INTEGRATED RECONFIGURABLE AVIONICS

For the reasons discussed above, ϕ_M will not be dealt with explicitly. Instead, the special structure of ϕ_M

which has been observed in proposed ICNIA architectures will be exploited to allow more efficient computations.

We assume that the system can be described by either a one-level or two-level structure. A one-level structure consists of a set of k-of-n modules in series. These k-of-n modules will be referred to as pools. The number of components (k) required in a pool depends on the function requirements. Pools which are irrelevant (i.e., k equal to zero) with respect to certain functions are allowed.

A two-level structure consists of a set of one-level structures. Each one-level structure will be referred to as a chain. Chains are either in "series" in the sense that all functions must use the chain, or "parallel" in the sense that a set of functions is supportable if there exists an allocation of functions to parallel chains such that each chain can support its functions. Parallel chains need not be identical; in particular, some functions may be restricted to certain chains.

Two slight generalizations to this model are also considered. First, pools may be described by real-valued capacities instead of integer-valued numbers of components. Any homogeneous Markov chain can be used to describe the degradation of pool capacity as a failure process. This extension allows system resources that undergo partial failures to be modeled. Second, the allocation of functions to parallel chains may not be strict in that pools may be shared between parallel chains. For example, processing resources in parallel chains may be shared if they communicate through data buses.

A.3 POOL CAPACITY COMPUTATIONS

For the pools in a single chain, let

C_i = capacity of pool i

u_{ij} = utilization by function j of pool i

$c_{max,i}$ = maximum capacity of pool i (no failures)

We now define two types of pools, according to how functions combine. If a set CF of critical functions is required simultaneously, the total requirement for pool i is

$$r_i = \begin{cases} \sum_{j \in CF} u_{ij} & \text{if pool } i \text{ is contending} \\ \max_{j \in CF} u_{ij} & \text{if pool } i \text{ is noncontending} \end{cases} \quad \text{(A-1)}$$

If the functions are not required simultaneously, all pools are considered noncontending. Pool capacities may represent the number of identical components in a pool which are functioning, the number of signals that can be multiplexed in a single component, or the available processing rate.

The exponential failure time distribution implies that C_i is a homogeneous Markov chain with some transition probability matrix (tpm) P^i. If a pool consists of identical components (each having a capacity of one), then its tpm is

$$P^i_{k\ell} = \begin{cases} \binom{k}{\ell} q^{k-\ell} (1-q)^{\ell} & , \quad k \geq \ell \\ 0 & \text{otherwise} \end{cases} \quad \text{(A-2)}$$

where

$q = e^{-\lambda t}$

t = mission length

λ = component failure rate

Mission Completion Success Probability (MCSP), defined as the probability that the set of functions CF is available throughout a mission, is just

$$\text{MCSP} = \prod_i \Pr\{C_i \geq r_i\} \quad \text{(A-3)}$$

which can be easily computed from the P^i and the initial system state distributions.

A.4 CHAIN STRUCTURE COMPUTATIONS

We now consider a two-level structure containing more than one chain. The computations are illustrated only

for the case of two chains in parallel. Pools are divided into the following types:

F: chain-fail pools (noncontending)

S: shared pools

N: noncontending pools, excluding types F and S

C: contending pools, excluding types F and S

A pair of pools, one in each chain, is type S if their resources can be used by functions allocated to the opposite chain. Type F pools are those which, upon failure, prevent the type S pools in the chain from being utilized. Type F pools also have the same utilization by all functions; hence, when they fail, the entire chain fails. The remaining pools are classified as type N or C according to Equation A-1. If functions are not required simultaneously, type C pools are treated as type N.

The state of a chain as determined by its pool capacities implies the ability to support certain functions. Let

$$X_j^k = \begin{cases} 1 & \text{if function } j \text{ can be supported on the type N pools on chain } k, \\ 0 & \text{otherwise} \end{cases}$$

$$\underline{X}^k = [X_j^k], \quad j \epsilon CF$$

$UP^k(t)$ = the event that the set of functions CF can be supported on the type t pools on chain k

$UP^{1+2}(t)$ = the event that the set of functions CF can be supported on the type t pools on the pair of parallel chains

for k = 1, 2 and t = F, S, N, C. The event $UP^{1+2}(C)$ is dependent upon $\underline{X}^k$ in that an allocation of functions to chains that is supportable on the type C pools must be consistent with the supportability of functions on the type N pools. Similarly, the event $UP^{1+2}(S)$ is dependent on $UP^k(F)$. Applying these definitions,

$$MCSP = Pr\{UP^{1+2}(F,S,N,C)\}$$

$$= Pr\{UP^{1+2}(C) | UP^{1+2}(N)\} \cdot Pr\{UP^{1+2}(N)\}$$

$$\cdot Pr\{UP^{1+2}(S) | UP^{1}(F), UP^{2}(F)\} \cdot Pr\{UP^{1}(F)\}\ Pr\{UP^{2}(F)\}$$

$$+ Pr\{UP^{1}(S,N,C)\} \cdot Pr\{UP^{1}(F)\} \cdot [1 - Pr\{UP^{2}(F)\}]$$

$$+ Pr\{UP^{2}(S,N,C)\} \cdot Pr\{UP^{2}(F)\} \cdot [1 - Pr\{UP^{1}(F)\}] \qquad (A\text{-}4)$$

The three terms in Equation A-4 correspond to both chains being up with respect to type F pools, chain one being up and chain two being up.

To evaluate the first term we condition on $\underline{X}^k$:

$$Pr\{UP^{1+2}(C) | UP^{1+2}(N)\} \cdot Pr\{UP^{1+2}(N)\}$$

$$= \sum_{\underline{x}^1 + \underline{x}^2 \geq \underline{1}} Pr\{UP^{1+2}(C) | \underline{X}^1 = \underline{x}^1, \underline{X}^2 = \underline{x}^2\} Pr\{\underline{X}^1 = \underline{x}^1\} Pr\{\underline{X}^2 = \underline{x}^2\} \qquad (A\text{-}5)$$

The distribution of $\underline{X}^k$ is determined by applying the single-chain analysis of Section A.3 to the type N pools for all subsets of the functions CF, giving $Pr\{\underline{X}^k \geq \underline{x}\}$ for all $\underline{x}$. The law of total probability is then used to obtain $Pr\{\underline{X}^k = \underline{x}\}$.

The type C pools are treated as follows. We assume that type C pools occur in pairs, one on each chain, and use the index i to refer to pairs rather than individual pools. A superscript will be used to indicate chain (e.g., C_i^k, $c_{max,i}^k$). The utilizations u_{ij}, however, are assumed to be the same for both chains. The allocation of functions to chains is represented by

$$y_j = \begin{cases} 1 & \text{if function j uses chain 1} \\ 0 & \text{if function j uses chain 2} \end{cases}$$

$$\underline{y} = [y_j], \quad j \epsilon CF$$

Let

$$r_i(\underline{y}) = \sum_{j \varepsilon CF} y_j \, u_{ij} \qquad \text{(A-6)}$$

The conditional event in Equation A-5 occurs if there is some allocation $\underline{y}$ such that

$$\underline{1} - \underline{x}^2 \leq \underline{y} \leq \underline{x}^1 \qquad \text{(A-7a)}$$

$$r_i(\underline{y}) \leq C_i^1 \qquad \text{(A-7b)}$$

$$r_i(\underline{1} - \underline{y}) \leq C_i^2 \qquad \text{(A-7c)}$$

for all type C pools i. That is, functions can be assigned only to chains on which the type N pools can support them, and the total function requirements must not exceed the type C pool capacities.

A necessary condition for such an allocation to exist is

$$r_i(1-\underline{x}^2) \leq C_i^1 \qquad \text{(A-8a)}$$

$$r_i(1-\underline{x}^1) \leq C_i^2 \qquad \text{(A-8b)}$$

$$r_i(\underline{1}) \leq C_i^1 + C_i^2 \qquad \text{(A-8c)}$$

$$\max_{j \varepsilon CF} u_{ij} \leq \max \{C_i^1, C_i^2\} \qquad \text{(A-8d)}$$

for all type C pools i. The probability of condition A-7 will be approximated by the probability of condition A-8. To motivate this approximation, note that condition A-8c requires that sufficient resources be available to perform the required functions. Errors occur in this approximation only in the probability that the required resources will be divided in unusable proportions on the two chains. In the case where there is only one type C pool pair i, $u_{ij} = 1$ and C_i^k takes on integer values, A-7 is equivalent to A-8a-c. Condition A-8d addresses the case of some u_{ij} being very large. Hence the approximation is reasonable.

Using Equation A-8 and assuming C_i^k is integer-valued,

$$\Pr\{UP^{1+2}(C) | \underline{X}^1 = \underline{x}^1, \underline{X}^2 = \underline{x}^2\}$$

$$\doteq \prod_{i \in C} \sum_{c^1=k}^{c^1_{max,i}} \Pr\{C_i^1 = c^1\} \cdot \Pr\{C_i^2 \geq \ell\} \qquad \text{(A-9)}$$

where

$$k = \max\{r_i(\underline{x}^1),\ r_i(\underline{1}) - c^2_{max,i}\}$$

$$\ell = \begin{cases} \max\{r_i(\underline{x}^2),\ r_i(\underline{1}) - c^1\} & \text{if } c^1 \geq \max\limits_{j \in CF} u_{ij}, \\ \max\{r_i(\underline{x}^2),\ r_i(\underline{1}) - c^1,\ \max\limits_{j \in CF} u_{ij}\} & \text{otherwise} \end{cases}$$

The type S pools are treated as follows. We assume that type S pools occur in pairs, one on each chain, and use the same notation as for type C pools. Because the paired resources are shared, we need consider only the combined capacity of the two pools:

$$\Pr\{UP^{1+2}(S) | UP^1(F),\ UP^2(F)\} = \prod_{i \in S} \Pr\{C_i^1 + C_i^2 \geq r_i(\underline{1})\}$$

$$= \prod_{i \in S} \sum_{c^1=r_i(\underline{1})-c^2_{max,i}}^{c^1_{max,i}} \Pr\{C_i^1 = c^1\}\ \Pr\{C_i^2 \geq r_i(\underline{1}) - c^1\}$$

(A-10)

Applying the single-chain analysis to the type F pools gives $\Pr\{UP^k(F)\}$. Combined with Equations A-5, A-9 and A-10, this completes the evaluation of the first term of Equation A-4.

To evaluate the second and third term, only $\Pr\{UP^k(S,N,C)\}$ is needed. It is obtained by applying the single-chain analysis to the type S, N and C pools for the set of functions CF. Note that if not all functions in CF are supported on chain k then $\Pr\{UP^k(S,N,C)\} = 0$.

Equation A-4 gives MCSP for a pair of parallel chains. If the system contains several chains or parallel chain sets in series, with reliabilities $MCSP_i$, the combined reliability is

$$MCSP = \prod_{\text{chains } i} MCSP_i \qquad \text{(A-11)}$$

A.5 MEAN TIME BETWEEN CRITICAL FAILURE ALGORITHM

Another measure which can be computed by MIREM is Mean Time Between Critical Failure (MTBCF), defined as the expected operating time without repair until a critical function is lost, starting with full system capacity. Let MCSP(t) be the weapon system reliability for an operating time of t hours. Then

$$MTBCF = -\int_0^\infty t \, dMCSP(t)$$

$$= \int_0^\infty MCSP(t)dt \qquad \text{(A-12)}$$

This integral is evaluated in MIREM using the trapezoidal rule with a variable step size which can be modified by exploration. Letting F(t) = MCSP(t), the algorithm proceeds as follows.

1. Select α, δ, ε_{min}, ε_{rel} and t_1. Initialize $t_o = 0$, $dt = t_1 - t_o$, $k = 1$.

$$\lambda_1 = \ln[\bar{F}(t_o)/\bar{F}(t_1)]/dt$$

$$\Delta = [\bar{F}(t_o) - \bar{F}(t_1)]dt/2$$

$$MTBCF = \Delta$$

2. $dt(\delta) = 0.8\delta \, dt/(\Delta \, \lambda_k)$

3. If $k \leq 2$, $dt = \min\{\alpha\ dt, dt(\delta)\}$.

If $k > 2$, $dt(\varepsilon_{rel}) = \left| 8\bar{F}(t_{k-1})(0.8\varepsilon_{rel}) / \frac{d^2\bar{F}}{dt^2} \right|^{1/2}$

and $dt = \min\{\alpha\ dt, \max\{dt(\delta), dt(\varepsilon_{rel})\}\}$.

4. $k = k + 1$.

5. $t_k = t_{k-1} + dt$

$$\frac{d^2\bar{F}}{dt^2} = 2\left[\frac{\bar{F}(t_k)-\bar{F}(t_{k-1})}{t_k - t_{k-1}} - \frac{\bar{F}(t_{k-1})-\bar{F}(t_{k-2})}{t_{k-1} - t_{k-2}}\right] \Big/ (t_k - t_{k-2})$$

$$\lambda_k = \ln[\bar{F}(t_{k-1})/\bar{F}(t_k)]/dt$$

$$\Delta = [\bar{F}(t_{k-1}) - \bar{F}(t_k)]dt/2$$

6. If $\varepsilon_{rel} < (dt)^2 \frac{d^2\bar{F}}{dt^2} / [8\bar{F}(t_{k-1})]$

and $\delta < \Delta\ \lambda_k$ then set $dt = dt/2$ and go to step 5.

7. $MTBCF = MTBCF + \Delta$

8. If $\bar{F}(t_k)/\lambda_k > 0.1$

and $\varepsilon_{min} < \frac{|\lambda_k - \lambda_{k-1}|}{\lambda_k(t_k - t_{k-1})}$

then go to step 2. Otherwise, set

$MTBCF = MTBCF + \bar{F}(t_k)/\lambda_k$

and stop.

This algorithm is based on the assumption that, at least for large t, $\bar{F}(t)$ can be approximated by $ae^{-\lambda t}$. Local estimates of λ serve as a basis for selecting a step size, $dt(\delta)$, which will include the desired fraction δ of the entire integral. Estimates of λ are also used as a stopping criterion. If the relative change in λ is less than ε_{min} per unit change in t, it is assumed that the remainder of $\bar{F}$ has a constant failure rate and it is integrated analytically. The parameter ε_{rel} provides an alternative basis for increasing the step size, based on the average relative error in $\bar{F}$ calculated from its second derivative. The scaling parameter α sets a limit on how rapidly step size can increase.

The parameters values that were used in this study are

$$\alpha = 4$$

$$\delta = 0.025$$

$$\varepsilon_{min} = 0.00005 \text{ hrs}^{-1}$$

$$\varepsilon_{rel} = 0.005$$

$$t_1 = 3 \text{ hrs}$$

Tests indicate that the MTBCF accuracy obtained using these values is better than 0.5%, while an average of only 22 function evaluations was required. These results suggest that the algorithm is more efficient for the life distributions considered than a general purpose routine.

A.6 SIMULATION OF OPERATIONAL AVAILABILITY/READINESS (SOAR) RELIABILITY INPUTS

The MCSP capability of MIREM also serves as a basis for computing the reliability inputs used in the Simulation of Operational Availability/Readiness (SOAR) model to evaluate deferred maintenance policies. In particular, we consider a maintenance policy of repairing only after missions in which critical failures occur and of replacing all LRUs which contain failures. The SOAR inputs are:

$MCSP(t;\tau)$ = the probability of completing a mission of length t with no critical failures for a system that has operated τ hours since repair with no critical failures

$R_C(\tau,\tau+t)$ = the probability that an LRU consisting of the set of components C contains a failure $\tau + t$ hours after repair given that a critical failure occurred between τ and $\tau + t$.

Both the weapon system reliability and the probability of pulling an LRU depend on the time since repair because of the build-up of noncritical failures.

Following Reference 8, let

T_i = operating time since repair at which component i fails

T_C = time of first failure in the set of components C

T_S = time at which a critical failure occurs in the system

$\underline{F}(\cdot)$ = vector distribution function of $[T_i]$

$\bar{\underline{F}}(\cdot) = \underline{1} - \underline{F}(\cdot)$

$h(\cdot)$ = system (i.e., critical failure) reliability function

$(1_C,\underline{x})$ = the vector $\underline{x}$ with all components in the index set C replaced by 1.

These definitions allow us to represent conditional failure probabilities (see also Reference 24):

$$h(\bar{\underline{F}}(t)) = \Pr\{T_S > t\} \qquad \text{(A-13.a)}$$

$$h(1_C,\bar{\underline{F}}(t)) = \Pr\{T_S > t | T_C > t\} \qquad \text{(A-13.b)}$$

In these terms

$$\begin{aligned} MCSP(t;\tau) &= \Pr\{T_S > \tau + t | T_S > \tau\} \\ &= \Pr\{T_S > \tau + t\}/\Pr\{T_S > \tau\} \\ &= MCSP(\tau + t)/MCSP(\tau) \end{aligned} \qquad \text{(A-14)}$$

and

$$R_C(\tau,\tau+t) = Pr\{T_C \leq \tau + t | \tau < T_S \leq \tau + t\}$$

$$= 1 - \frac{Pr\{\tau < T_S \leq \tau + t | T_C > \tau + t\} Pr\{T_C > \tau + t\}}{Pr\{\tau < T_S \leq \tau + t\}}$$

$$= 1 - \frac{[h(l_C,\underline{\bar{F}}(\tau)) - h(l_C,\underline{\bar{F}}(\tau+t))]\bar{F}_C(\tau+t)}{h(\underline{\bar{F}}(\tau)) - h(\underline{\bar{F}}(\tau+t))} \qquad \text{(A-15)}$$

To evaluate Equation A-15 using MIREM, we observe that

$$\bar{F}_C(t) = Pr\{T_C > t\}$$

$$= \prod_{i \varepsilon C} e^{-\lambda_i t} \qquad \text{(A-16.a)}$$

$$h(\underline{\bar{F}}(t)) = MCSP(t) \qquad \text{(A-16.b)}$$

and that $h(l_C,\underline{\bar{F}}(t))$ can be evaluated in the same fashion as $h(\underline{\bar{F}}(t))$ if we first set $\lambda_i = 0$ for $i \varepsilon C$.

APPENDIX B

GLOSSARY

A/J	Anti-jam
BIT	Built-In Test
CNI	Communication, navigation and identification
GPS	Global positioning system
HF	1. High frequency, 2. HF clear voice communication set, AN/ARC-190
ICNIA	Integrated communication, navigation and identification avionics
IFFI	Identify friend-or-foe, interogator set, AN/APX-76B
IFFT	Identify friend-or-foe, transponder set, AN/APX-101
ILS	Instrument landing system, AN/ARC-108
JTIDS	Joint tactical information distribution system
LCC	Life-cycle cost
LRU	Line replaceable unit
MCSP	Mission completion success probability
MIREM	Mission reliability model
MTBCF	Mean time between critical failure
MTBF	Mean time between failure
MTTR	Mean time to repair
RFI	Ready for issue spare part
R/R	Remove and replace maintenance action
SDU	Secure data unit

SEEK TALK	UHF anti-jam voice communication set (to be replaced by HAVE CLEAR)
SINCGARS	Single channel ground and airborne radio subsystem
SOAR	Simulation of operational availability/readiness
SRU	Shop replaceable unit
TACAN	Tactical air navigation set, AN/ARN-118
UHF	1. Ultra-high frequency, 2. UHF clear voice communication set, AN/ARC-164
VHF	1. Very high frequency, 2. VHF clear voice communication set, AN/ARC-186